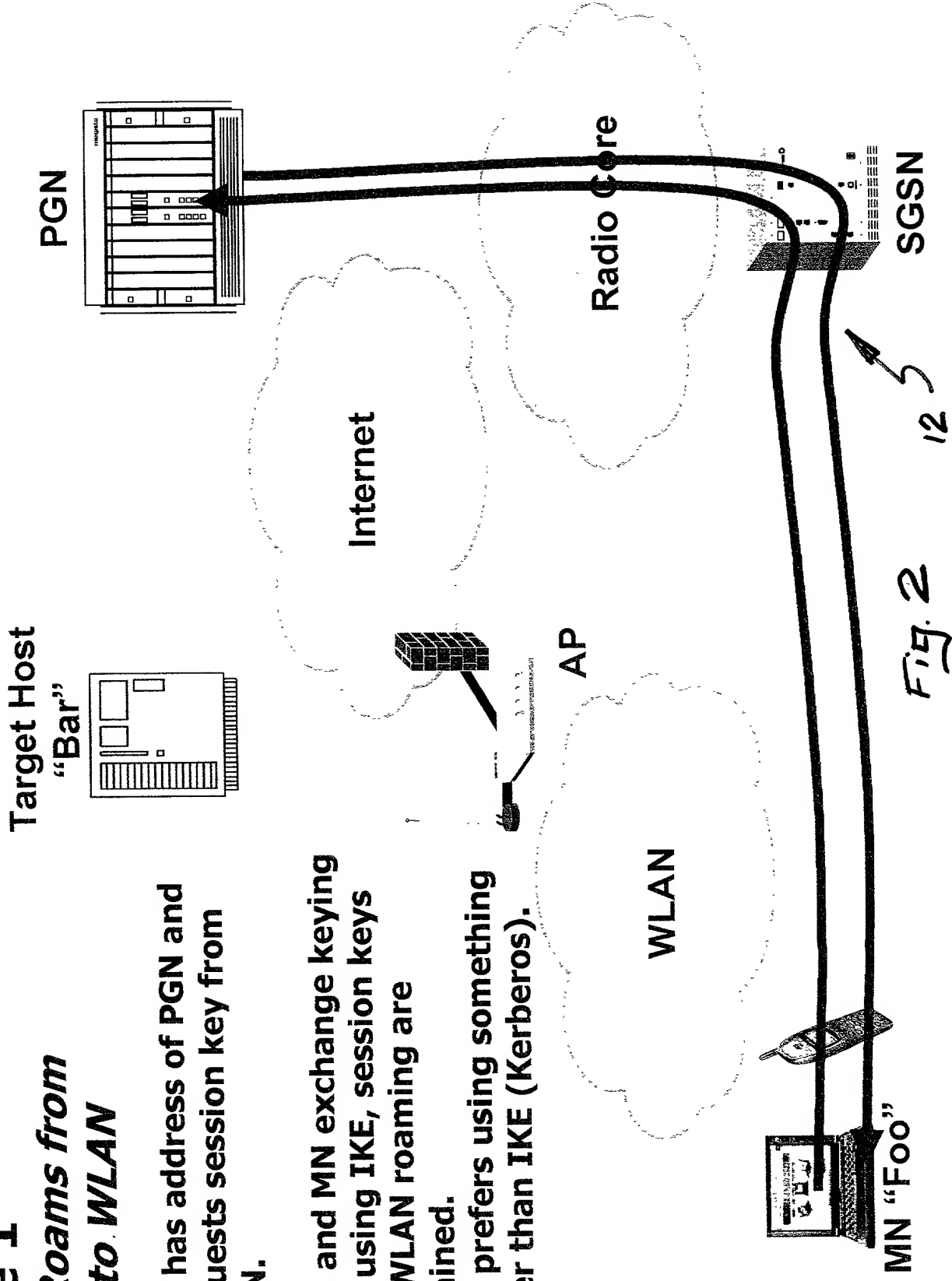


Fig. 1

Phase 1

User Roams from GPRS to WLAN

1. MN has address of PGN and requests session key from PGN.
- PGN and MN exchange keying info using IKE, session keys for WLAN roaming are obtained.
 - Luis prefers using something other than IKE (Kerberos).



Phase 2

1. MN shows up on WLAN and requests local care-of-address from DHCP
2. MN gets care-of-address

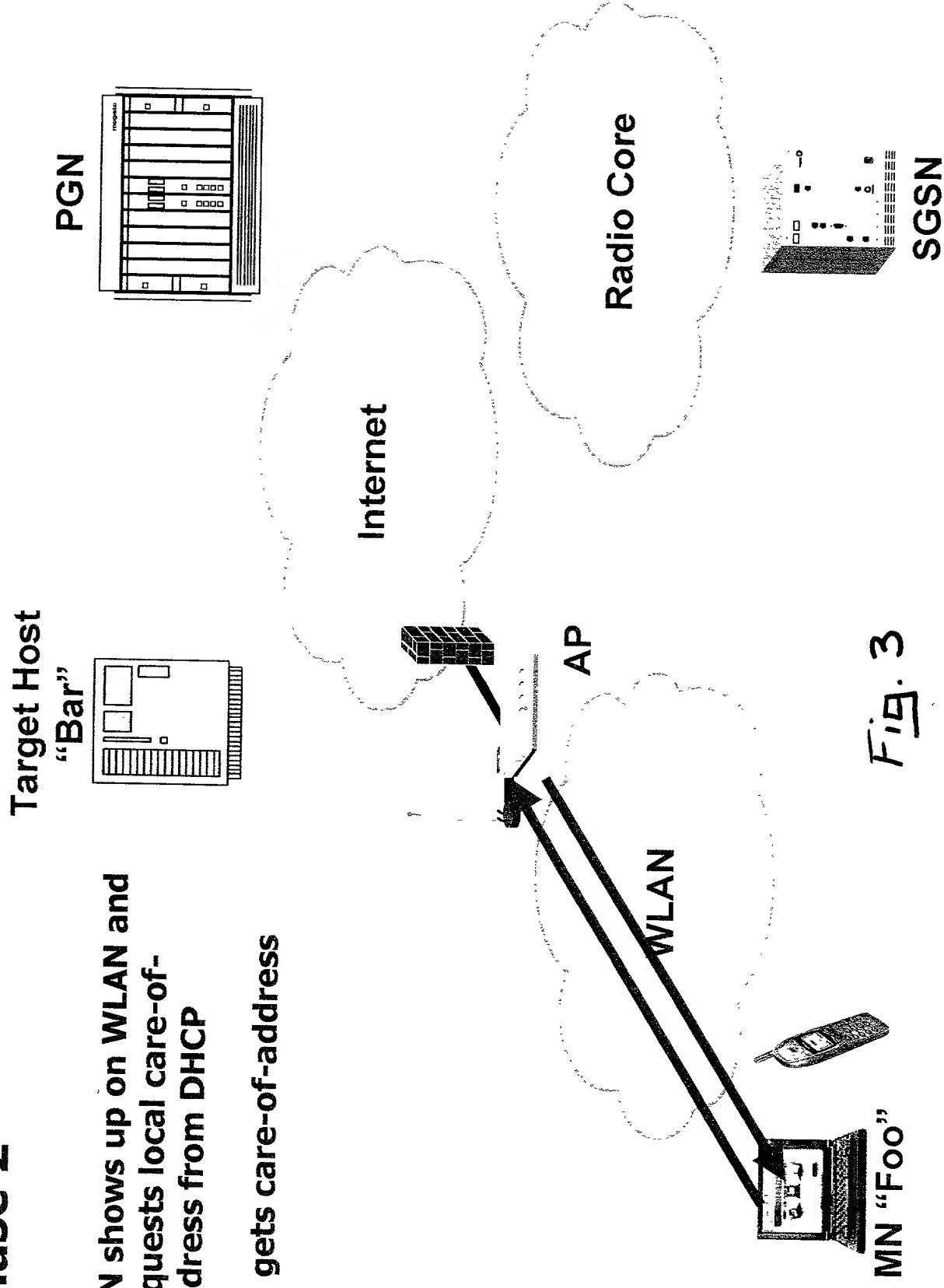


Fig. 3

Phase 3

1. MN sends a Mobile IP (MIP) registration request to the home agent (HA) hosted in the PGN
 - HA sends registration reply (request and reply sent secured using session key)
 - IKE used to set up IPSEC tunnel established between PGN and MN using COA (auth, encrypted, MICed)

Target Host
"Bar"

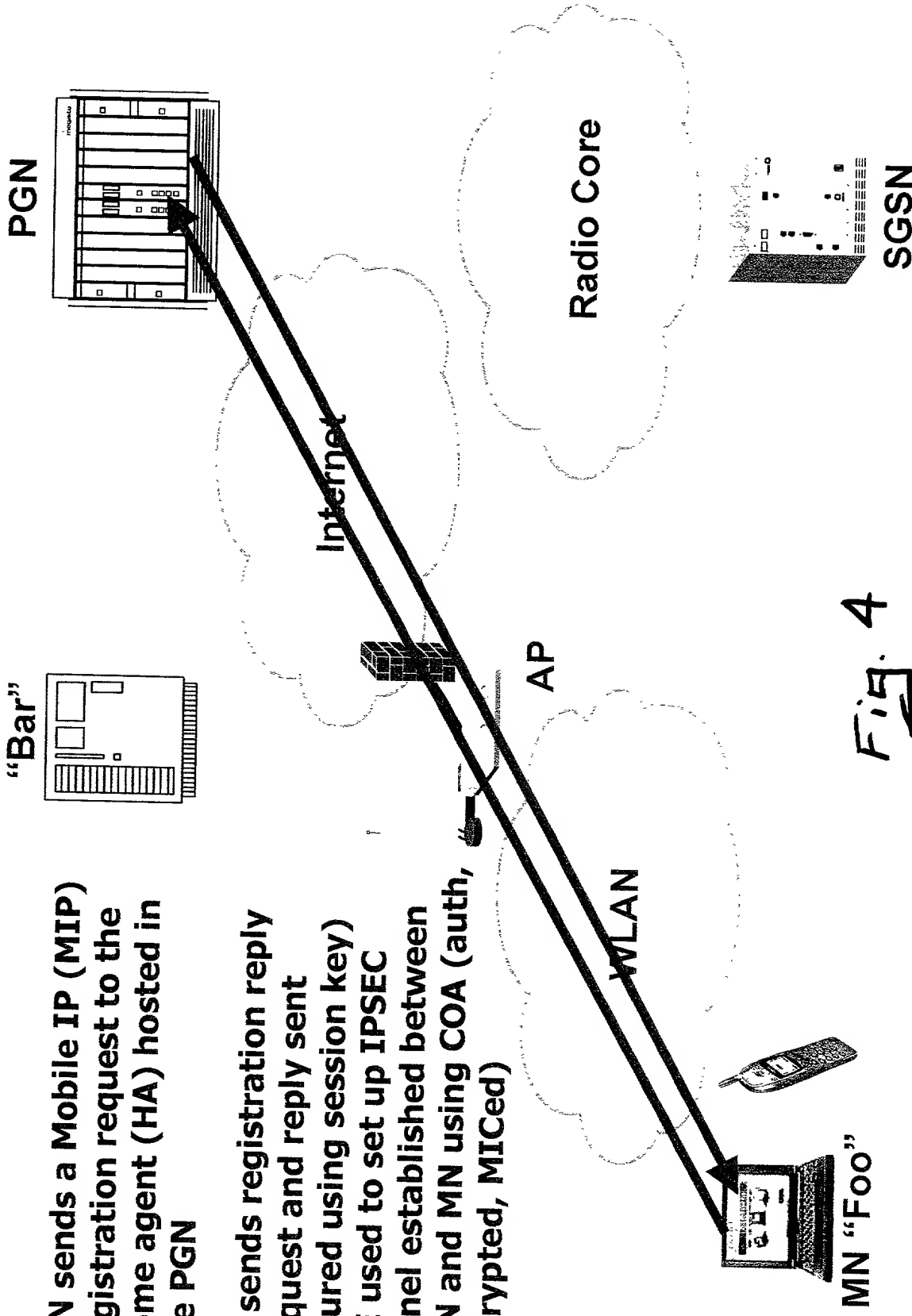


Fig. 4

Phase 4

1. MN Foo sends pkts to Bar via HA reverse IPSEC tunnel.
2. Bar sends packets to Foo via the HA in forward IPSEC tunnel.

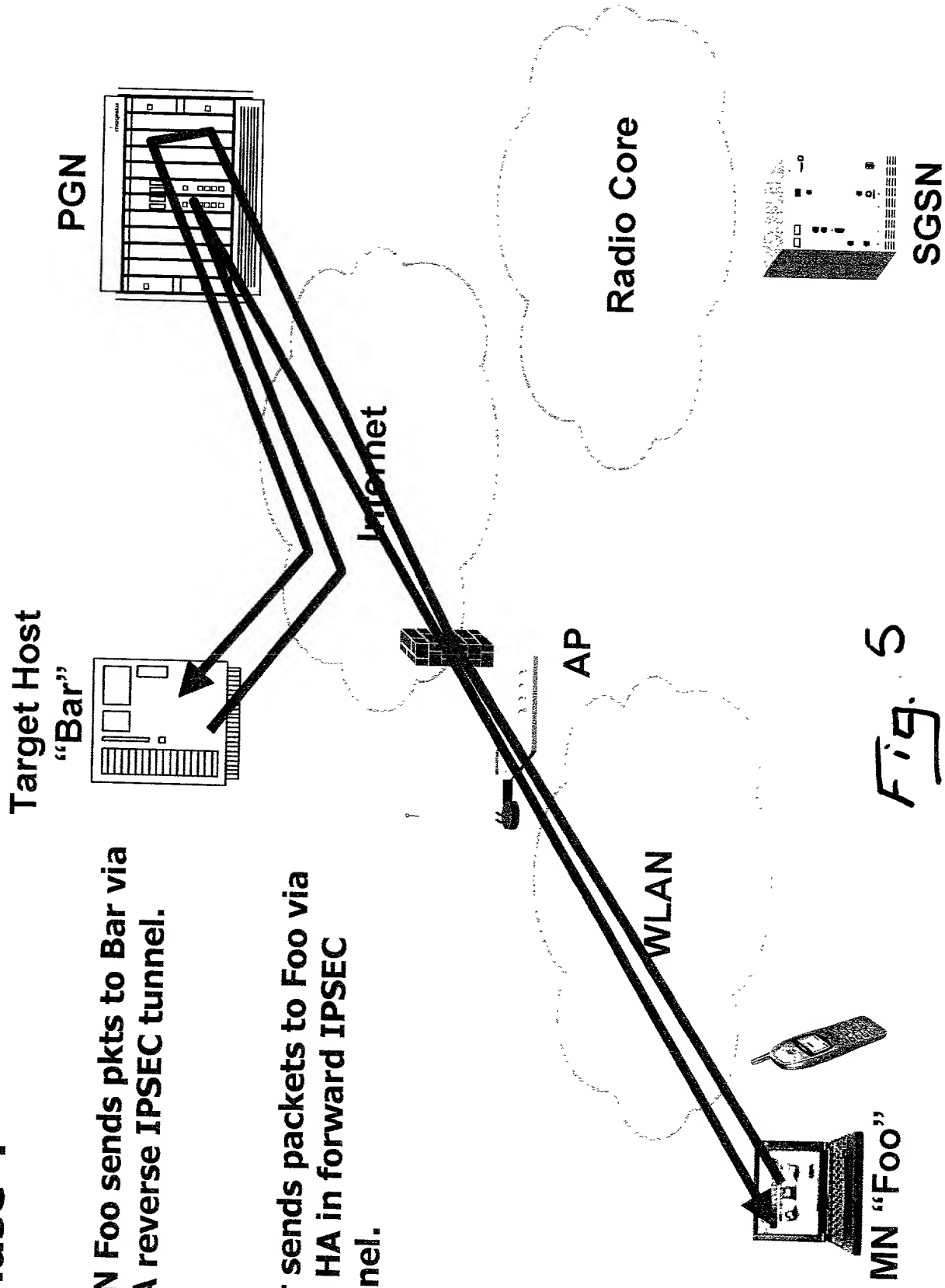


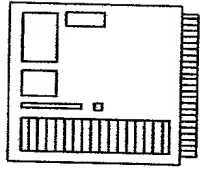
Fig. 5

Phase 5

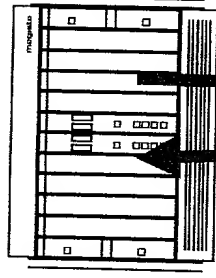
User Roams from WLAN to GPRS

- MN foo sends MIP registration request to HA using authentication info generated from session key to say that it is back on home network.
- 2. HA sends MIP registration reply back to MN Foo.

Target Host
"Bar"



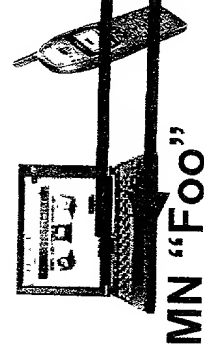
PGN



Internet

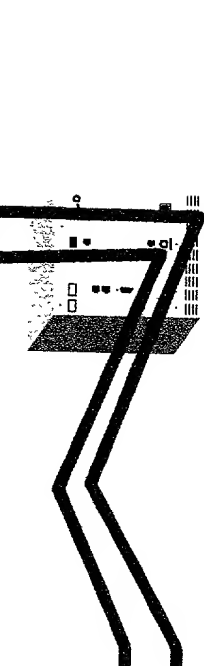
Radio Core

Fig. 6



MN "Foo"

SGSN



Phase 6

1. Packets from Foo to Bar now go via GPRS only.
2. Packets from Bar to Foo now go via GPRS only.

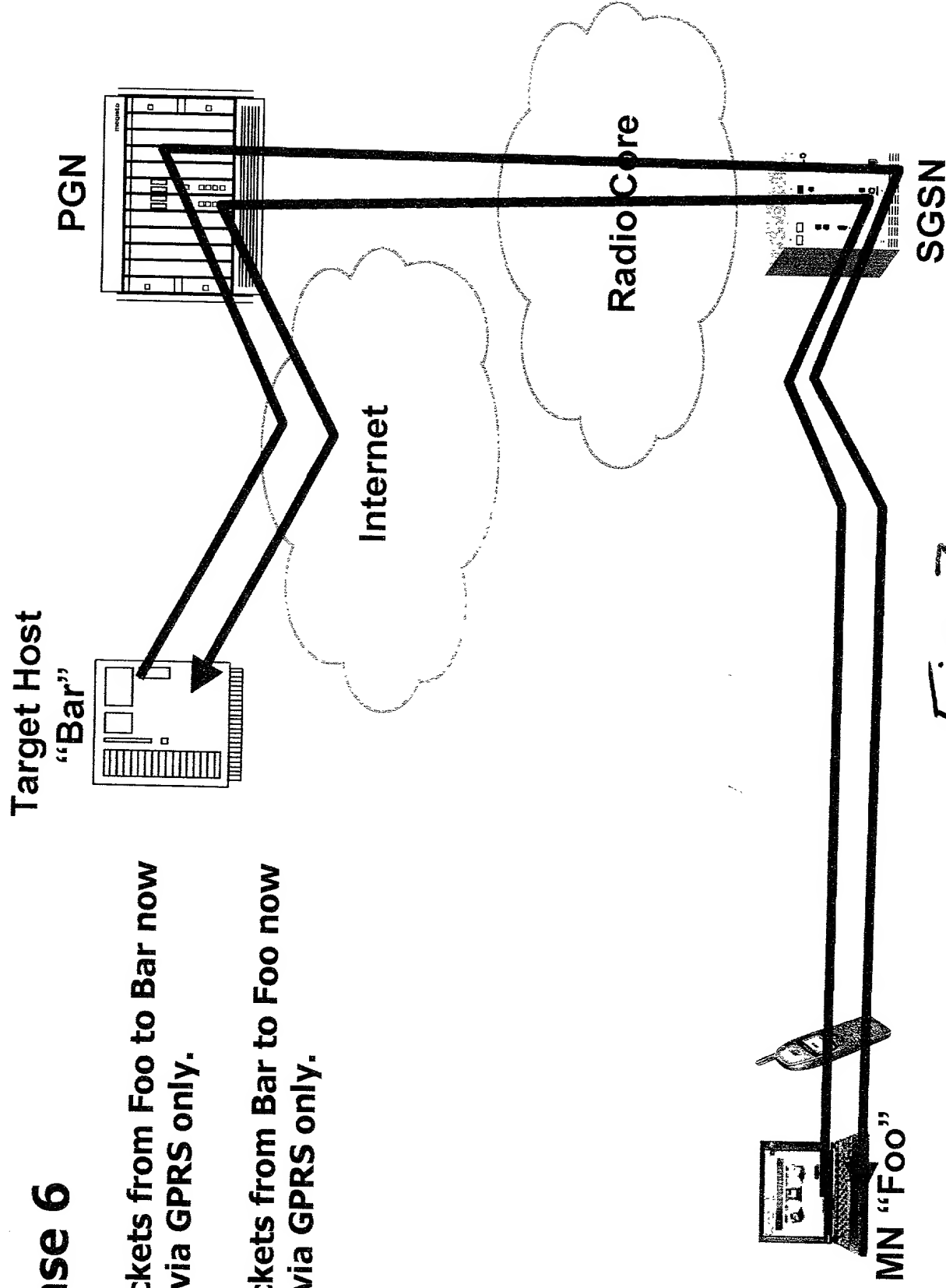


Fig. 7

A key exchange is performed across the GPRS / UMTS network between the MN 1 and the PGN 7 to establish a shared secret key.

80

PGN 7 performs an MD-5 hash to provide a 128-bit authentication value for use in the Mobile IP protocol.

82

MN 1 establishes a connection on Wireless LAN 3 and requests a Mobile IP Care-Of-Address (COA) from a Dynamic Host Configuration Protocol (DHCP) server on the Internet.

83

Fig. 8A

The MN 3 receives the COA across the Wireless LAN 3.

84

MN 1 performs an MD-5 hash of the key obtained to obtain a 128-bit authentication value for use in the Mobile IP protocol.

85

MN 1 sends a Mobile IP registration request to the Home Agent (HA) hosted in the PGN 7 using the authentication value established. If the MN 1 has activated the SA (an IPsec ESP tunnel) with the PGN 7, the registration messages can be sent in an encrypted form.

88

To Figure 8B

